EGBA | European Gaming & Betting Association

Guidance document on a proper implementation of the Fourth Anti-Money Laundering Directive

July 2017

Contents

Introduction 3

1. The low risk level of online gambling 3

1.1 General remarks 3

1.2 Online gambling operators' efforts 4

1.3 EU, private operators and national regulators' efforts 5

1.4 The low degree of vulnerability of applicable transactions 5

2. The use of strict Customer Due Diligence requirements 6

2.1 General remarks on the implementation of the CDD process 6

2.2 The timing of the CDD process 8

2.3 Specific requirements for customers 8

3. Costs and impacts incurred by gambling services providers when implementing AML measures 9

4. Conclusion 9

Introduction

We, the European Gaming and Betting Association (**"EGBA"**), the association representing the leading online cross-border licensed gaming and betting operators in the European Union (**"EU"**), present this guidance document on the transposition of the Fourth Anti-Money Laundering Directive (hereinafter the **"Directive"**)[1].

The main objective of this note is to provide Member States with guidance and clear recommendations for an effective transposition of the provisions contained in the Directive. EGBA would thus like to share our expertise and knowledge to ensure a safe and sustainable anti-money laundering regulatory framework across the EU.

Firstly, we will focus our comments on the low risk nature of online gambling linked to the 4th AMLD provisions setting out a possibility for exemption (**1**). Secondly, we will elaborate on the Customer Due Diligence (hereinafter **"CDD"**) requirements (**2**). Lastly, we will conclude by highlighting the costs and impacts incurred by gambling services providers when implementing the Directive (**3**).

1. The low risk level of online gambling

Article 2(2) of the Directive provides for the possibility for Member States to define, in the national legislation, exemptions to certain proven low risk gambling activities, which will have to be notified to the European Commission together with a justification based on the specific risk assessment. In their risk assessment, Member States shall assess the degree of vulnerability of the applicable transactions, including with respect to the payment methods used.

With regards to this provision, we first consider that online gambling in general does not constitute a high risk activity in terms of money laundering (**1.1**), not only due to transparency efforts made by gambling operators (**1.2**), but also due to the overall efforts made by the EU, private operators and national regulators (**1.3**). The low risk nature of online gambling is supported by money laundering prevention measures taken by online gambling operators concerning more specifically payment methods (**1.4**)

1.1 General remarks

First, we would like to point out that, due to a number of reasons on which we will elaborate below, online gaming and betting does not present high risks in terms of money laundering. This view has been shared by the European Commission, which has stated the following:
"*As for money laundering, there is currently very limited information or evidence suggesting that licensed online gambling operators in Europe are subject to money laundering activities. The prevailing problem is linked to unregulated operators who are offering their services at a distance from outside of the EU with either no or a very low degree of regulation and supervision"*[2].

[1] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 05/06/2015.
[2] Commission Staff Working Document 'Online gambling in the Internal Market' accompanying the Communication from the Commission to the European Parliament, the Council, the Economic and Social

Furthermore, already in 2009, a study carried out by Professor Levi, from the University of Cardiff, found that:
"*There is much mythology about e-gaming laundering risks, fed by inadequate information and a tendency to project a dislike of gaming and/or private sector involvement in it into alarm about e-crime in general and the role of gaming in this*"[3].
"*In short, compared to methods of customer identification and monitoring in the offline gaming and financial services sector, the scope for substantial abuse of e-gaming for laundering purposes is modest, both for those crimes that generate cash and for those that do not'*"[4].

Those comments are also underpinned by all the practical means deployed by online gambling actors to fight against money laundering (below).

1.2 Online gambling operators' efforts

The low risk level of online gambling and betting in terms of money laundering is due to the traceability of all gambling activities and transactions. This transparency is, for instance, ensured by the recording and tracking of all customer transactions by the operators.

In particular, the paragraphs below describe part of the **direct and pro-active strategy** undertaken by EU licensed and regulated operators. This strategy involves comprehensive and continuous mitigation work on the industry risk-factors, with particular efforts around:

- **Transactions**: entirely cash-free transaction system integrated with the highly regulated EU financial services providers.
- **Visibility**: complete lack of customer anonymity, where gambling CDD processes are personalised in line with the accounts themselves.
- **Closed loop**: it must be shown that the customer owns any financial instrument used to deposit/withdraw money.
- **Audited Internal Control Systems**: operators employ advanced Internal Control Systems (hereinafter **"ICS"**) built on a risk-based approach and the flagging of suspicious activity for further enhanced customer due diligence. Measures such as deposit blocks and account suspensions are taken when deemed necessary.
- **Accountability**: online gambling operators use cutting-edge technology processes and routine operations which are inherently highly traceable and easily audited (i.e. digital fingerprints, tracking of detailed customer action trail from log-in to log-out).
- **Training**: for every employees, according to their specific duties, more particular, to those directly monitoring AML and fraud risks, on the practical issues, such as, the characteristics of the suspicions, how to escalate them to the compliance officer and further information about how to tackle the issues on an operational level.

Moreover, national legislation in all Member States already imposes strict Know-Your-Costumer (hereinafter **"KYC"**) requirements on online operators. These requirements aim at the verification of

Committee and the Committee of the Regions 'Towards a comprehensive framework for online gambling' {COM(2012) 596 final}, 23.10.2012, p. 89.
[3] Money Laundering Risks and E-Gaming: A European Overview and Assessment, Final Report, Michael Levi, Ph.D., D.Sc. (Econ.), Cardiff University, September 2009, p. 6.
[4] *Ibidem*, p. 26.

the identity of players, and oblige online gambling operators to request and verify a number of documents for each of their players[5].

1.3 EU, private operators and national regulators' efforts

The risk of gambling-related money-laundering is becoming even lower, in recent years, due to the actions taken in the field of electronic verification by EU and national regulators, and by private operators.

Concerning the public sector, initiatives are being taken in order to improve/harmonize **electronic identification systems and procedures**. These initiatives include for instance, the eIDAS Regulation[6], or the issuing of e-ID cards by some Member States such as Spain, Estonia and Belgium.
Regarding the private sector, companies more and more are launching **identity verification services**. Examples of that are BankID[7] in the Nordics or webID[8].

Moreover, it is worth mentioning that **consumer trust is a key asset for online gambling operators**, which seek to be distinguished by consumers in what relates to, *inter alia*, gambling-related crime prevention. **Most consumers are reluctant to play with operators believed to be linked with criminal or terrorist organizations**. For this reason, private operators have also put in place developed initiatives to bring the fight against fraud one step beyond.

For instance, the CEN Workshop Agreement on responsible remote gambling measures (2011) obliges EU regulated operators to constantly monitor and report suspicious transactions to the relevant authorities. The CEN Workshop Agreement, which includes more than one hundred measures dealing mostly with consumer protection and fraud and gambling-related crime prevention, is based on a recommendation on online gambling issued by the European Commission on 2014[9].

1.4 The low degree of vulnerability of applicable transactions

Nowadays most online gambling operators are cross-border and hold multiple licenses in multiple jurisdictions; they are therefore obliged to comply with a large number of rules for combatting money laundering, according to the license requirements established by each national regulator.

As a standard, **EU - licensed and regulated - online gambling providers**, due to the nature of the online service and in order to comply with the 4th AMLD, fraud prevention and responsible gaming standards, **do not operate with cash but rather through highly regulated financial institutions, adding an additional layer of security to their processes**. On the contrary, the use of cash by land-based gambling activities[10] does not require any registration or customer identification, leading some users to turn away from easily traceable digital payment options.

---

[5] For an extensive explanation of the KYC process please *see* EGBA's Online Gambling Regulation Manual, 24 May 2016, 3rd Edition, pages 4-9.
[6] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014.
[7] https://www.bankid.com/en/
[8] https://www.webid-solutions.de/en/
[9] Commission Recommendation of 14 July 2014 on principles for the protection of consumers and players of online gambling services and for the prevention of minors from gambling online, 2014/478/EU, OJ L 214, 19.7.2014.
[10] For eg., Europol published, on 9 March, the "EU Serious and Organised Crime Threat Assessment – Crime in the age of technology" (SOCTA 2017) which confirms that cash remains at the core of the money laundering

Please find below a table including information from one of our members on the payment methods used by customers to make a deposit:

Deposit methods	Split per frequency	Split per amount
Bank	0.1%	0.5%
Cards	49.1%	51.1%
eWallet	2.5%	7.8%
Instant	42.5%	37.2%
Prepaid	5.8%	3.3%
Grand Total	100.0%	100.0%

Further, it should be reminded that **gambling transactions over the internet are traceable, recorded and transparent due to the digital footprint** (presenting fewer risks than cash payments or face-to-face identification) and hence offer far more possibilities to detect and prosecute fraudulent activities than offline transactions.

Recommendation 1
While Article 2(2) of the 4th AMLD provides for the possibility for Member States to exempt certain proven low risk gambling activities, we do not consider it as necessary or advisable to seek any exemption for any specific gambling activity. Online gambling operators usually do not make any differentiation in procedures between the provision of online gaming and online betting products but apply appropriate AML procedures to all of these products equally. Such a choice is justified also by practical reasons: when offering a wide range of both online gaming and online betting products, allowing customers to use funds in their single wallets to gamble on all products is easier.
It would therefore be more sensible to assess risk by sector rather than by specific gambling activity

Recommendation 2
Taking into account the fact that most EU online gambling services providers operate through highly regulated financial institutions, it is therefore preferable, in our view, to only allow payment methods which are offered by Payment Service Providers licensed in the EU/EEA to ensure an additional level of supervision

2. The use of strict Customer Due Diligence requirements

Chapter II of the 4th AMLD focuses on the CDD process. The implementation of such measures leaves an important margin of discretion to Member States. We therefore would like to provide our guidance not only on the implementation of the process in general (**2.1**), on what constitutes in our view the optimal timing of the CDD process (**2.2**) and also on the specific requirements which apply to customers (**2.3**).

2.1 General remarks on the implementation of the CDD process

In our view, the aim of the CDD process is to mitigate the risks of fraud and money-laundering, consisting of two main steps: (i) obtaining information from the player and (ii) verifying the accuracy

business and one of the facilitators of most types of serious and organised crime in the EU (https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017).

of the information provided. It requires information such as name, date of birth, photo, address, contacts and national ID number. Afterwards, the operator will verify this information by using different methods depending on national legislations.

The most commonly used method, which is also recommended by the European Commission[11], **is a temporary grace period in which verification needs to be completed, but during in which the player is allowed to play**. A 30-day temporary account allows players to deposit money and play but not to withdraw any money, which is only possible after the completion of the CDD Process. If the player fails to successfully prove his/her information, the temporary account will be automatically closed. An alternative method would be to conduct verification once a player has reached a threshold (risk-based approach).

More generally, two important facts need to be taken into consideration. The first of them is that **CDD measures involve the processing of a significant amount of personal data.** In that regard and as stated in the 4th AMLD, CDD requirements must comply with Directive 95/46/EC (hereinafter **"Data Protection Directive"**)[12], and must observe the right to the protection of personal data of potential players[13].

The second of them is that **customer experience in any e-commerce sector, such as online gambling, plays a crucial role in channeling the demand towards the regulated offer**. It is therefore, also with regard to anti-money laundering measures, crucial to take into account that the demand needs to be channeled towards the regulated offer. Therefore, the CDD process should be convenient from a player's perspective, without being too burdensome, something that has been acknowledged by the European Commission[14]. Otherwise, there is a risk that the demand for online gambling services will be channeled towards the unregulated offer.

In order to effectively fight fraud, regulations should give operators the possibility to close or suspend accounts if fraudulent activity is suspected. This should be possible at any given time and for the duration until when the identity is verified and risk removed. Following the verification, if the operator still has doubts about fraudulent activity, the operator should reserve the right to cancel any deposits made, or temporarily confiscate any funds until the account has been verified or a chargeback has been received.

In any event, when designing CDD requirements it must be born in mind that operators are continuously having to balance and navigate through risk of conflicting legal obligation (i.e. data protection), operational feasibility (legislation against what is technically and operationally possible and financially sustainably feasible).

Recommendation 3

We consider that the implementation of CDD requirements is most effective when it takes into account the protection of personal data of players and the customers' experience as it is an element of utter importance when it comes to the channeling of consumers towards the regulated offer.

In order to make the CDD process easier, and as recommended by the European Commission, we are also of the opinion that national authorities should facilitate online gambling operators' access to

[11] EC 2014 Recommendation, paragraph 22.
[12] Data Protection Directive, Article 41(1).
[13] Data Protection Directive, Recital 65.
[14] EC 2014 Recommendation, paragraph 21.

"national registers, databases or other official documents against which operators should verify the identity details"[15].

2.2 The timing of the CDD process

Article 11(d) of the 4th AMLD provides that:

"*Member States shall ensure that obliged entities apply customer due diligence measures in the following circumstances:*

(d) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;"

In order to implement this disposition, we would like to give our definition of the terms "wagering a stake" and "collection of winnings". "**Wagering of a stake**" means depositing money, as customers usually have to wager their money before they make a withdrawal; and "**collection of winnings**" means withdrawals from the gambling wallet to the customers preferred payment method.

When defining those terms, it would be sensible from Member States to link the criteria to a time period. In our view, only real cash flows should be considered, when determining at what point of time a customer has reached the EUR 2000 threshold giving rise to the CDD process.

2.3 Specific requirements for customers

It is important to note that it is **common practice amongst all regulatory regimes for customers to be only allowed to have one account**. In case this rule is breached, the operator reserves the right, according to its Terms and Conditions (TAC), to block and/or delete the extra account held by the player and to reallocate all the funds to a single account. A single player is not permitted to open multiple accounts with the same operator. The exception to this rule is if the accounts are on different brands that the operator is able to link in the back end.

Further, some regulated operators have introduced **an obligation for the player's account name to match the name of the payment card or other payment methods used to deposit/withdraw funds**. Depending on the national framework, the operator may carry the verification of the bank account with the respective financial entity. For instance, IP address tracking can be used to identify the location of customer deposits/withdrawals and gaming activity. Exceptionally, operators would pay out winnings to a different account than the one used to deposit money into the account only if the deposit payment method does not support withdrawals back to that same account.

Finally, the player's account is non-transferable, meaning that it is prohibited for players to sell, assign, transfer or acquire accounts from or to other players. The player shall not allow any other individual to use his or her account, access or use any material or information from the operator's website, accept any prize or participate in the services.

As to the use of "dirty funds", it should be noted that most funds that are credited to gaming accounts are already in the banking system, meaning that they are in general transferred from a bank account. If that is not the case (i.e. paysafecard), operators have controls in place to restrict winnings and additional

[15] EC 2014 Recommendation, paragraph 18.

checks are made before players can withdraw when they have only done limited or no playing activity, because this is flagged as a suspicious activity.

Recommendation 4
The CDD process should take place when real money transactions take place in the gambling operators' wallet

3. Costs and impacts incurred by gambling services providers when implementing AML measures

The 4th AMLD, being a Directive, its implementation into national law may lead to duplication with existing AML legislation. Therefore any harmonization would be likely to increase efficiency and reduce costs. In general, remote operators make high levels of financial and resource investments to support strong compliance and monitoring functions. This is due to stringent regulation that applies to the online gambling sector and to the fact that, as stated above, consumer trust is a key asset for online gambling operators. Operators make substantial investments in order to avoid being involved in any financial scandal.

However, we do not believe that the extension of the anti-money laundering regime to online betting would incur significant costs, especially due to the fact that in practice, EU licensed and regulated operators' approach towards online betting already takes into account the anti-money laundering national legislations.

4. Conclusion

The 4th AMLD represents a crucial pan-European instrument to fight money laundering and to establish harmonised rules across the EU Member States regarding which EGBA believes it is necessary for the national legislative framework to lay the appropriate foundations.

It is therefore of utmost importance that Member States bring into force the provisions of the 4th AMLD by 26 June 2017 while taking the necessary measures to enable operators to tackle and detect fraudulent transactions in the best possible manner in order to maintain the safety and integrity of the online gambling environment. EGBA also counsels against unnecessary gold plating, which would not achieve practical results but may hinder the channelling effect.